

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:	)	Examiner: Abbaszadeh, Jaweed A.
Matthew J. WAGNER, et. al.	)	
	)	Art Unit: 2115
Serial No.: 10/780,397	)	
	)	
Filed: 02-17-2004	)	Confirmation No.: 1613
	)	
For: Computer Security System and	)	
Method	)	
	)	
Date of Final Office Action:	)	Attorney Docket No.:
June 25, 2008	)	
	)	200314073-1

March 6, 2009

**APPEAL BRIEF**

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is timely provided within one month of the Pre-Appeal Brief Decision mailed February 6, 2009.

**1. Real Party in Interest:**

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

**2. Related Appeals and Interferences**

There are no other prior and/or pending appeals, interferences, or judicial proceedings that are related to, directly affect, or that will be directly affected by or have a bearing on the Board's decision.

**3. Status of Claims**

Claims 1-46 are pending in the application.

Claims 1-46 stand rejected.

No claims were canceled.

No claims were allowed.

No claims were withdrawn.

The rejections of claims 1-46 are appealed.

**4. Status of Amendments**

No Amendments were filed subsequent to the Final Office Action.

## 5. Summary of Claimed Subject Matter

Appellant notes that citations that include paragraph numbers and line numbers (e.g. [0020], lines 1-4) refer to line numbers starting at the top of the paragraph, not at the top of the page.

### Independent Claim 1

Claim 1 recites a computer security system with a self-managed device (specification, page 2-3, paragraph [0012] lines 5-11; Figure 1, self-managed device 90); the device has an authentication system for controlling access to the self-managed device by a user (specification, page 2-3, paragraph [0012] lines 5-11; Figure 1, self-managed device 90). Additionally, claim 1 recites a security module adapted to authenticate an identity of the user (specification page 6, paragraph [0021] lines 5-9 and Figure 1, authentication system 110). In response to the user authentication, the module automatically generates device credential data verifiable by the authentication system to enable user access to the self-managed device, where the generating is transparent to the user (specification, page 4, paragraph [0015] lines 3-9; Figure 1, security module 44).

### Independent Claim 11

Claim 11 recites a computer security system with a means for controlling user access to a self-managed device. One structure that corresponds to the claimed function of controlling is credential validator 120 (see specification page 6, paragraph [0021] lines 7-11 and Figure 1, credential validator 120). The system recited in claim 11 can include a means for authenticating an identity of the user. One structure that corresponds to the claimed function of authenticating is security module 44 (specification, page 4, paragraph [0015] lines 2-3; Figure 1, security module 44). The means for authenticating automatically generates, transparently to the user, device credential data in response to the user authentication; the device credential data is

verifiable by the authentication system to enable user access to the self-managed device (specification, page 4, paragraph [0015] lines 3-9; Figure 1, security module 44).

Independent Claim 16

Claim 16 recites a method that includes authenticating an identity of a user. (specification, page 12, paragraph [0039] lines 9-11; Figure 4, block 416) Additionally, the method of claim 16 includes automatically generating device credential data that is transparent to the user in response to user authentication (specification, page 4, paragraph [0015] lines 3-9; Figure 1, security module 44 - specification, page 12, paragraph [0039] lines 11-12; Figure 4, block 418). The device credential data is verifiable by an authentication system of a self-managed device to enable user access to the self-managed device (specification, page 4, paragraph [0015] lines 3-9; Figure 1, security module 44 - specification, page 12, paragraph [0039] lines 11-12; Figure 4, block 418).

Independent Claim 25

Claim 25 recites a computer security system that includes a security module executed by a processor (specification, page 6, paragraph [0021] lines 2-3; Figure 1, security module 44). The security module adapts to access credential data to verify an identity of a user (specification, page 4, paragraph [0015] lines 3-9; Figure 1, security module 44). Moreover, the system of claim 25 recites an activation/deactivation module that is accessible via a networked administration client (specification, page 8-9, paragraph [0027] lines 1-4; Figure 1, activation/deactivation module 140). The activation/deactivation module is adapted to interface with the security module in response to a request by the administration client to activate, transparently to the user, an authentication system of a self-managed device to control user access to the self-managed device (specification, page 9, paragraph [0028] lines 1-7; Figure 1, activation/deactivation module 140).

Independent Claim 31

Claim 31 recites a computer network security system that comprises a security module adapted to automatically generate device credential data verifiable by an authentication system of a self-managed device to enable user access to the self-managed device; the device credential data is transparently to the user (specification, page 4, paragraph [0015] lines 3-9; Figure 1, security module 44). The system of claim 31 also comprises an activation/deactivation module adapted to receive a request from the user to automatically activate the authentication system of the self-managed device (specification, page 7, paragraph [0022] lines 8-14; Figure 1, activation/deactivation module 140).

Independent Claim 37

Claim 37 recites a computer security method that includes authenticating an identity of a user (specification, page 12, paragraph [0039] lines 9-11; Figure 4, block 416). If the authentication is successful, then the method generates and transmits device credential data to a self-managed device in a manner transparent to the user. The device credential data is for authentication by the self-managed device to enable the user to access the self-managed device (specification, page 4, paragraph [0015] lines 3-9; Figure 1, security module 44 - specification, page 12, paragraph [0039] lines 11-12; Figure 4, block 418).

Independent Claim 42

Claim 42 recites an electronic device with a self-managed device located within the electronic device. The self-managed device is configured to manage user access to the self-managed device. (specification page 6, paragraph [0021] lines 5-11 and Figure 1, credential validator 120). A security module is disposed within a basic input/output system (BIOS) of the electronic device (specification, page 4, paragraph

[0015] lines 9-12; Figure 1, BIOS 40). The security module configures to automatically generate device credential data verifiable by an authentication system of the self-managed device; the automatic generation occurs in response to user authentication and is transparent to the user (specification, page 4, paragraph [0015] lines 3-8; Figure 1, security module 44).

## **6. Grounds of Rejection to be Reviewed on Appeal**

I. Whether claims 1-46 are unpatentable under 35 U.S.C. §102(e) as being anticipated by Yeates et al. (US 2005/0125698).

## 7. Argument

### **I. Whether claims 1-46 are unpatentable under 35 U.S.C. §102(e) as being anticipated by Yeates et al. (US 2005/0125698).**

The Final Office Action (“FOA”) did not address the substantive rejections of the claims based on the reference. Rather it incorporated the rejections and rationale of the Non-Final Office Action (“NFOA”) issued on 1-29-08 (FOA page 2, paragraph 4). The Final Office Action only addressed the §1.131 declarations filed on 3/12/2008, which the examiner deemed ineffective to overcome the Yeates reference. Both actions are considered relevant in the present arguments.

Appellant respectfully submits that independent Claims 1, 11, 16, 25, 31, and 37, and Claims 2-10, 12-15, 17-24, 26-30, 32-36, and 38-46 that depend respectively therefrom, are patentable over Yeates. Yeates does not qualify as prior art under Section 102(e) and, therefore, no *prima facie* rejection has been made.

#### **Submitted Declarations under 37 CFR 1.131**

37 CFR 1.131(a) allows an applicant to “submit an appropriate oath or declaration to establish invention of the subject matter of the rejected claims prior to the effective date of the reference”. Declarations and Exhibits were submitted under 37 CFR 1.131 by the Applicant on March 10, 2008. Thus these documents are in the record and are not attached to the present appeal brief. The submitted declarations and exhibits establish the invention of the claimed subject matter under 1.131(a) and establish “conception of the invention prior to the effective date of the reference coupled with due diligence from prior to said date to a subsequent reduction to practice or to the filing of the application” under 1.131(b).

The submitted declarations are appropriate in the present case because the conditions of 37 CFR 1.131(a)(1) and (2) do not exist. In particular, the present

claims and the claims of Yeates do not claim the same patentable invention under 37 CFR 1.131(a)(1). This is determined by a simple review of the claimed elements. Also, the present rejections are not based upon a statutory bar since Yeates is applied under 35 USC §102(e). Thus the present declarations are not excluded under 37 CFR 1.131(a)(2).

A. Declarations establish invention of the subject matter of the rejected claims

Exhibit A from the declaration of Matthew J. Wagner is an “Invention Disclosure” form completed and submitted by the inventors prior to the December 5, 2003 filing date of Yeates. The Final Office Action (FOA) alleges that exhibit A fails to prove conception of the invention (FOA, page 4). Thus the examiner did not remove Yeates as prior art. The examiner is incorrect.

Exhibit A does establish invention of the subject matter of the rejected claims as required by 37 CFR 1.131(a). Using present claim 1 as a representative claim, it recites:

1. A computer security system, comprising:
  - a self-managed device having an authentication system for controlling access to the self-managed device by a user; and
  - a security module adapted to authenticate an identity of the user and, in response to user authentication, automatically generate, transparently to the user, device credential data verifiable by the authentication system to enable user access to the self-managed device.

Each element of claim 1 is now addressed.

The “computer security system” preamble

On page 5 of exhibit A, it discloses an invention relating to and for “computer systems” and “authentication mechanisms” (page 5, first paragraph). It also discloses “a security subsystem” (page 5, last paragraph). Thus a “computer security system” of claim 1 is disclosed and supported by the evidence.

The “self-managed device” element

Exhibit A discloses: “...“device” or “devices”) incorporate self-managed authentication mechanisms that require a user credential (e.g. a password) as a condition for access.” (page 5, 1<sup>st</sup> paragraph, lines 1-3). Thus the recited “self-managed device having an authentication system for controlling access to the self-managed device by a user” is clearly disclosed.

The “security module” element

Exhibit A discloses:

When access to the protected device is required, the security subsystem would first authenticate the user or other requestor. Successful authentication would then allow the above-created password to be decrypted and used to access the protected device.

(page 5, last paragraph)

Thus the claimed feature of “a security module adapted to authenticate an identity of the user” is clearly disclosed. The remaining language of the claim starting with “in response to ...” is also clearly disclosed. One of ordinary skill in the art would clearly understand that after “successful authentication” (e.g. in response to user authentication), a password is decrypted and then used to access the protected device (e.g. “the self-managed device”). The action of decrypting a password involves generating different values or different data from the original password. It is

known in the art that decrypting an object results in a different object. Hence this is a “generating” action that discloses and supports the claimed automatically generating function. Although the exhibit discloses a specific example of decrypting a password, it is common to generalize components when they are claimed. A password is one example of and is covered by the claimed “device credential data”. The exhibit affirmatively correlates the two terms in page 5, 1<sup>st</sup> paragraph, lines 2-3 where it states, “a user credential (e.g. a password)”.

The automatic and transparent features are disclosed and supported by for example: “This Invention Disclosure describes a method to automate the enablement of such self-managed authentication features with little to no user interaction.” (page 5, 3<sup>rd</sup> paragraph, lines 1-2). This is what automatic and transparent means.

It is well known that patent claims are legalese drafted by an attorney. Claims are drafted from disclosed materials received from an inventor. The present claims were clearly drafted from the subject matter disclosed in exhibit A. Inventors do not draft claim language and it is not a requirement that the exact claim language be found in the exhibits. The applicant’s burden is to show that the “subject matter” of the claim is disclosed. As seen above, exhibit A clearly establishes that “the subject matter” of the invention is disclosed as required by 37 CFR 1.131(a). Therefore, the present Exhibits and Declarations comply with 37 CFR 1.131 and establish invention of the subject matter of the rejected claims prior to the effective date of the Yeates reference. Yeates should be removed as a reference and thus a *prima facie* rejection has not been established. The rejection should be reversed.

B. Conception of the invention and due diligence under 37 CFR 1.131(b)

The Declarations and Exhibits submitted on March 10, 2008 included the Declarations of Matthew J. Wagner (the “Wagner Declaration”), Valiuddin Ali (the “Ali Declaration”) and Manuel Novoa (the “Novoa Declaration”) under 37 C.F.R. §1.131,

together with exhibits thereof. These documents evidence the conception of the invention prior to the purported effective date of *Yeates* and diligence in the completion of the invention, which is the subject of the present Application from a time prior to the purported effective date of *Yeates* continuously up to the date of filing of the present Application.

Also submitted on March 10, 2008 was the declaration of James L. Baudino (the "Baudino Declaration") under 37 C.F.R. § 1.131. James L. Baudino, who is a registered patent attorney, was responsible for supervising/Preparing and filing the present Application. The Wagner Declaration alone or in combination with the Ali Declaration, the Novoa Declaration, and/or the Baudino Declaration evidences diligence in the completion of the invention which is the subject of the present Application from a time prior to the purported effective date of *Yeates* continuously up to the date of filing of the present Application. The above-referenced declarations and evidence submitted therewith evidence the conception of the invention prior to the purported effective date of *Yeates* coupled with reasonable diligence from a time before the purported effective date of *Yeates* and continuously up to the filing of the present Application.

The Court of Customs and Patent Appeals, predecessor court to the Federal Circuit, has held that diligence is shown when a patent attorney has a typical practice of reviewing draft patent applications in sequence based on the chronological order in which they are received. *Gould v. Schawlow*, 363 F.2d 908 (CCPA 1966). Moreover, a patent attorney is not required to drop all other work and concentrate on a particular invention. "If the attorney has a reasonable backlog of unrelated cases which he takes up in chronological order and carries out expeditiously, that is sufficient" to establish reasonable diligence. MPEP 2138.06, sixth paragraph "DILIGENCE REQUIRED IN PREPARING AND FILING PATENT APPLICATION".

In view of these legal precedents, appellant submits that the Baudino Declaration, alone or in combination with the Wagner Declaration, the Ali Declaration

and/or the Novoa Declaration, are sufficient to demonstrate reasonable due diligence from a date prior to December 5, 2003 to the filing of the present application on February 17, 2004.

The FOA did not contest or reject the submitted evidence of due diligence. Thus it is assumed that the examiner accepted that the present facts demonstrate due diligence.

Based on the facts, the examiner erred in not applying the submitted declarations and erred in not removing Yeates as prior art. Appellant respectfully requests that the rejection of Claims 1-46 based on Yeates be reversed.

### **Yeates Fails to Anticipate the Claims**

Claims 1-46 were rejected in the NFOA and FOA based upon Yeates (NFOA, page 2, section 2, paragraph 1 and FOA page 2, paragraph 4). Of the rejected claims, Claims 1, 11, 16, 25, 31, and 37 are independent. Claim 1 will be discussed as a representative claim.

Yeates relates to a simple storage system where data is retained as one of two types: application user data or sensitive system data (Yeates, paragraph [0028], lines 4-6). Claim 1 recites in part “a security module adapted to authenticate an identity of the user and, in response to user authentication, automatically generate, transparently to the user, device credential data verifiable by the authentication system to enable user access to the self-managed device.” Yeates fails to disclose, teach, or suggest this element.

It appears the NFOA combines two aspects of Yeates in an attempt to show that Yeates teaches the claimed security module element. The first aspect is a hash algorithm to protect a password on a computer system, which is combined with a

second aspect of providing a key to a user once there is authentication of user identity (NFOA, page 2, section 2, paragraph 4). Combination of these two aspects still fails to teach or suggest the claimed element.

In the first aspect, Yeates discloses "...when a password is registered for the first time, a one-way encryption hash of the password phrase is produced and persisted in the database." (Yeates, paragraph [0033], lines 3-6). Therefore, Yeates discloses creating a hash upon registering a password. This process relates to a password registration process and is not part of a user access process, which occurs when a user attempts to access sensitive data. The NFOA erroneously contends that the password registration process and the hash relate to generation of device credential data in response to user authentication (NFOA, page 2, section 2, paragraph 4).

In the second aspect, Yeates discloses that a user enters a username and password and a comparison is made between the user entered information and stored records (Yeates, paragraph [0032] lines 4-9). This is the user access step. If the comparison results in showing that the user is authorized, then the user can be permitted to access an application shared encryption key (ASEK) that is used for accessing data (Yeates, paragraph [0027], lines 7-8 and Yeates, paragraph [0032], lines 13-17). The combination of these two aspects fails to disclose, teach, or suggest each and every element of claim 1.

The aspects of Yeates used in the NFOA to reject claim 1 substantially differ from what is recited in claim 1. First, Yeates fails to disclose "a security module adapted to...in response to user authentication, **automatically generate, transparently to the user**, device credential data" (emphasis added) as recited in claim 1. The NFOA states that Yeates' hash is equivalent to the device credential data (NFOA, page 2, section 2, paragraph 4). Even if the hash of Yeates is equivalent to the device credential data of claim 1, which Appellant denies, there is no

mention in Yeates on hash generation being transparent. The rejection is improper for at least this reason and should be reversed.

Secondly, claim 1 recites “a security module adapted to authenticate an identity of the user and, ***in response to user authentication***, automatically generate...device credential data...” (emphasis added). In Yeates, a password is registered and then a hash created. This occurs during a password registration process. At a later time, a user attempts to access the system and provides a password. If the password is verified, access to the ASEK is provided (Yeates, paragraph [0032]).

Assuming the comparison shows that the user is authorized to utilize the application, then the user is able to access his/her version of the ASEK, which can then be used to access and/or store data in association with sensitive system data 304.

(Yeates, paragraph [0032], last sentence)

Therefore upon authentication/verification of the password, the ASEK is not generated. Rather, Yeates discloses that the resulting function is that “access” is provided to the previously generated ASEK. Thus no new data is generated automatically “in response to user authentication” as recited in claim 1. Furthermore, the previously discussed hash is not generated during this step in Yeates. Rather, the hash is produced during the password registration process and thus is irrelevant to the claim. Accordingly Yeates fails to teach or suggest automatically generating device credential data in response to user authentication as recited in claim 1.

The NFOA contends that the hash of Yeates is equivalent to the claimed device credential data and cites to Yeates [0033] (NFOA, page 2, section 2, paragraph 4). However, Yeates [0033] clearly explains that the hash is produced “when a password is registered for the first time” ([0033], lines 3-5). Again, this paragraph discusses a password registration process, which is different from the user authentication process. Accordingly, the hash of Yeates is not automatically

generated “in response to user authentication” as recited in the claim. Therefore, paragraph [0033] is unrelated to the present claims and fails to teach or suggest the generating function. As explained above, during the user access process, Yeates discloses that access is provided to the ASEK in response to verification of a user password (last sentence of [0032]). Therefore, the Office Action has misinterpreted Yeates. The rationale of the rejection is incorrect and a *prima facie* anticipation rejection has not been established. The rejection should be reversed.

Additionally, claim 1 recites “a self-managed device having an authentication system for controlling access to the self-managed device by a user...” The Office Action does not address this claimed element and does not cite to any portion of Yeates that teaches this element (NFOA, page 2, section 2, paragraph 3). There is no specific citation on how Yeates anticipates the first element of claim 1, just a mere listing of the element. Therefore a *prima facie* anticipation rejection has not been established for this additional reason. The rejection is improper and should be reversed. Accordingly, the rejections are also improper for the remaining claims and should be reversed.

**Conclusion**

For the reasons set forth above, a prima facie anticipation or obviousness rejection has not been established for any claim. All rejections have been shown to be improper. Appellant respectfully believes that all pending claims **1-46** patentably and unobviously distinguish over the references of record and that the rejections should be withdrawn. Appellant respectfully requests that the Board of Appeals overturn the Examiner's rejections and allow all pending claims. An early allowance of all claims is earnestly solicited.

Respectfully submitted,



---

Peter Kraguljac (Reg. No. 38,520)

(216) 503-5500  
Kraguljac & Kalnay, LLC  
Summit One, Suite 510  
4700 Rockside Road.  
Independence, OH 44131

## 8. Claims Appendix

1. A computer security system, comprising:
  - a self-managed device having an authentication system for controlling access to the self-managed device by a user; and
  - a security module adapted to authenticate an identity of the user and, in response to user authentication, automatically generate, transparently to the user, device credential data verifiable by the authentication system to enable user access to the self-managed device.
2. The system of Claim 1, wherein the security module is adapted to randomly generate the device credential data.
3. The system of Claim 1, wherein the security module is adapted to automatically transmit, transparently to the user, the device credential data to the self-managed device.
4. The system of Claim 1, wherein the security module is adapted to receive a request from a networked administration client to activate the authentication system of the self-managed device.

5. The system of Claim 1, wherein the security module is disposed within a basic input/output system (BIOS).

6. The system of Claim 1, wherein the security module is adapted to access relational data correlating the user to the device credential data for the self-managed device.

7. The system of Claim 1, further comprising an activation/deactivation module accessible by an administration client to activate the authentication system of the self-managed device.

8. The system of Claim 1, further comprising an activation/deactivation module accessible by an administration client to deactivate the authentication system of the self-managed device.

9. The system of Claim 1, wherein the security module is adapted to receive a request from a networked administration client to deactivate the authentication system of the self-managed device.

10. The system of Claim 1, wherein the security module is adapted to perform a registration operation to register the self-managed device.

11. A computer security system, comprising:
  - means for controlling user access to a self-managed device; and
  - means for authenticating an identity of the user and, in response to user authentication, automatically generating, transparently to the user, device credential data verifiable by the controlling means to enable user access to the self-managed device.
12. The system of Claim 11, further comprising means for automatically transmitting the device credential data, transparently to the user, to the self-managed device for verification by the controlling means.
13. The system of Claim 11, further comprising means for correlating the device credential data with the user.
14. The system of Claim 11, further comprising means for receiving a request from a networked administration client to activate the controlling means.
15. The system of Claim 11, further comprising means for randomly generating the device credential data.
16. A computer security method, comprising:
  - authenticating an identity of a user; and

automatically generating transparently to the user, in response to user authentication, device credential data verifiable by an authentication system of a self-managed device to enable user access to the self-managed device.

17. The method of Claim 16, further comprising automatically transmitting, transparently to the user, the device credential data to the self-managed device.

18. The method of Claim 16, further comprising randomly generating the device credential data.

19. The method of Claim 16, further comprising receiving a request from a networked administration client to activate the authentication system of the self-managed device.

20. The method of Claim 16, further comprising receiving a request from a networked administration client to deactivate the authentication system of the self-managed device.

21. The method of Claim 16, further comprising initiating an activation/deactivation module to enable activation of the authentication system.

22. The method of Claim 16, further comprising accessing relational data correlating the device credential data with the user.

23. The method of Claim 16, further comprising storing the device credential data at the self-managed device.

24. The method of Claim 16, further comprising performing a registration operation to register the self-managed device to the user.

25. A computer security system, comprising:

a security module executable by a processor, the security module adapted to access credential data to verify an identity of a user; and

an activation/deactivation module accessible via a networked administration client, the activation/deactivation module adapted to interface with the security module in response to a request by the administration client to activate, transparently to the user, an authentication system of a self-managed device to control user access to the self-managed device.

26. The system of Claim 25, wherein the security module is adapted to automatically generate, transparently to the user, a device credential for verification by the authentication system.

27. The system of Claim 25, wherein the security module is adapted to randomly generate, transparently to the user, a device credential for verification by the authentication system.

28. The system of Claim 25, wherein the security module is adapted to transmit, transparently to the user, a device credential to the device for verification by the authentication system.

29. The system of Claim 25, wherein the activation/deactivation module is adapted to display to the user registered self-managed devices available for authentication system deactivation.

30. The system of Claim 25, wherein the security module is adapted to correlate a device credential for verification by the authentication system with the user.

31. A computer network security system, comprising:  
a security module adapted to automatically generate, transparently to a user, device credential data verifiable by an authentication system of a self-managed device to enable user access to the self-managed device; and

an activation/deactivation module adapted to receive a request from the user to automatically activate the authentication system of the self-managed device.

32. The system of Claim 31, wherein the security module is adapted to automatically transmit, transparently to the user, the device credential data to the authentication system.

33. The system of Claim 31, wherein the self-managed device is adapted to store the device credential data received from the security module.

34. The system of Claim 31, wherein the security module is disposed within a basic input/output system (BIOS).

35. The system of Claim 31, wherein the activation/deactivation module is adapted to receive a request from a networked administration client to activate the authentication system.

36. The system of Claim 31, wherein the security module is adapted to randomly generate the device credential.

37. A computer security method, comprising:

authenticating an identity of a user; and  
if successfully authenticated, generating and transmitting, transparently to the user, device credential data to a self-managed device for authentication by the self-managed device to enable the user to access the self-managed device.

38. The method of Claim 37, further comprising correlating the identity of the user to the device credential data.

39. The method of Claim 37, further comprising performing a registration operation to register the self-managed device.

40. The method of Claim 37, further comprising encrypting the device credential data.

41. The method of Claim 37, wherein transmitting comprises transmitting, transparently to the user, encrypted device credential data to the self-managed device for decryption by the self-managed device to authenticate access to the self-managed device.

42. An electronic device, comprising:  
a self-managed device disposed within the electronic device and configured to manage user access to the self-managed device; and

a security module disposed within a basic input/output system (BIOS) of the electronic device and, in response to user authentication, configured to automatically generate, transparently to the user, device credential data verifiable by an authentication system of the self-managed device.

43. The electronic device of Claim 42, wherein the security module is configured to randomly generate the device credential data.

44. The electronic device of Claim 42, wherein the security module is configured to receive a request from a networked administration client to activate the authentication system of the self-managed device.

45. The electronic device of Claim 42, further comprising an activation/deactivation module accessible by an administration client to activate the authentication system of the self-managed device.

46. The electronic device of Claim 42, wherein the security module is configured to receive a request from a network administration client to deactivate the authentication system of the self-managed device.

**9. Evidence Appendix**

None. There is no extrinsic evidence.

**10. Related Proceedings Appendix**

None. There are no related proceedings.